

DRAFT

Version N.11

OSUNet Technical Standards and Operational Requirements

**Enterprise Networking
Office of Information Technology
The Ohio State University**

November 19, 2004

Index

1. General OSUNet Requirements

- 1.1 Overview**
- 1.2 OSUNet Connection Procedures**
- 1.3 OSUNet Host Connection Requirements**
- 1.4 Monitoring of the Network**
- 1.5 Protection of the Network**
- 1.6 Campus Border Port Blocking**
- 1.7 OSUNet Best Practices**
- 1.8 OSUNet Principles**
- 1.9 References**

2. Domain Name Service (DNS) Requirements

- 2.1 The osu.edu domain**
- 2.2 The ohio-state.edu domain**
- 2.3 Non ohio-state.edu domains**
- 2.4 Hosting DNS for TLDs on campus**
- 2.5 Windows Active Directory and DNS**
- 2.6 References**

3. Host Security Requirements

- 3.1 Installation Requirements**
- 3.2 Password Requirements**
- 3.3 Antivirus Requirements**
- 3.4 Auditing Requirements**
- 3.5 Additional Host Security Information**
- 3.6 References**

4. Network Security Requirements

- 4.1 Authentication Requirements**
- 4.2 Networking Devices**
- 4.3 Additional Network Security Information**
- 4.4 References**

5. Host Blocking and Unblocking Procedures

5.1 Notification about blocked hosts

5.2 Blocked Host Message

5.3 Unblocking a Host

5.4 Multiple Unblock Requests

5.5 Questions

5.6 References

6. Logging Requirements

6.1 References

7. Authentication Requirements

7.1 Requirements

7.2 Acceptable Forms of Authentication

7.3 References

8. Enforcement

8.1 Incidents that require an active response

8.2 Incidents that do not require an active response

8.3 References

9. Glossary

1. General OSUNet Requirements

1.1 Overview

The technical standards and operational requirements outlined in this document are designed to provide guidance for all academic and administrative units that desire to connect to OSUNet. Items outlined in these standards are requirements that must be met in order to receive and maintain an OSUNet network connection. Items that are recommended but are not specifically required are outlined in several “best practices” documents referenced throughout this document.

In collaboration with the campus technical user community OIT will periodically update these requirements for devices connected directly or through unit facilities to OSUNet, communications protocols supported on OSUNet, and both operational and security requirements for the use of OSUNet. The community will be represented by the PlanIT Stakeholders Group and the Ohio State University Network Working Group (NETWOG).

All decisions, notifications, or measures taken under these technical standards and operational requirements may be appealed to the CIO through the CIO Office Director of

Information Technology Policy and Services. Appeals are to be submitted by email to ITPolicy@osu.edu.

1.2 OSUNet Connection Procedures

1. All OSUNet connections are initiated by submitting an [application form \(PDF\)](#), with the appropriate financial commitments and approvals to the Director of Enterprise Networking, or his designee.
2. To receive and maintain an OSUNet connection the academic or administrative unit requesting the connection is required to have resources available to administer and trouble shoot their local network. [Minimum knowledge and skills a Department needs to receive an OSUNet connection](#)
3. To receive and maintain a connection to OSUNet the academic or administrative unit is required to identify both a Departmental Network Administrator (DNA) and one or more secondary network contacts. The person filling the role of DNA will act as the focal point for interfacing with OIT.

To register a DNA the person's name, phone number(s), office address, and name.n are to be provided to the university hostmaster (hostmaster@net.ohio-state.edu). While the specific job duties for a DNA are assigned by the employing academic or administrative unit, OIT has expectations that whoever is assigned the role will have at least a limited technical background and would be able to assist with first level network support for their users. To this end all DNAs are required to comply with the [Minimum Expectations of DNAs](#). (To determine the identity of your current DNA, an individual may contact the OIT help desk at 688-HELP (8help@osu.edu) or hostmaster@net.ohio-state.edu.)

4. DNAs will be allocated a range of IP addresses to meet their academic or administrative unit's needs. DNAs are responsible to administer that address space in conformance with the terms outlined in this document, along with any other responsibilities and guidelines imposed by their department or other university policies.
5. The secondary network contact(s) will be registered by OIT, and contacted in the event of a serious incident or if the primary DNA is unavailable. It is recommended but not required that the secondary network contact(s) meet the [Minimum Expectations of DNAs](#). To register these contacts the DNA for the network must provide the correct name.n and contact information to the university hostmaster (hostmaster@net.ohio-state.edu).

1.3 OSUNet Host Connection Requirements

The following requirements are the minimum steps that academic and administrative units must take to attach a [host](#) to OSUNet.

1. DNAs are required to register all *hosts* that use IP addresses in the OSUNet Domain Name System (DNS). Registration information needs to be sent to the university hostmaster, hostmaster@net.ohio-state.edu (Information and assistance is available from the [Hostmaster FAQ](#), or call 688-HELP). The university DNS requirements are outlined in Section 2 of this document

2. All *hosts* connected to OSUNet must comply with the patching and system maintenance requirements covered in the OSUNet Host Security Requirements and the Network Security Requirements that are outlined in Sections 3 and 4 of this document.

3. All academic and administrative units must develop and enforce policies for their area that ensure the timely application of operating system and other patches including the updating of anti-virus software, as well as the timely performance of other maintenance activities on university owned *hosts*. These policies must be applied to all university owned *hosts* that are connected to OSUNet.

Units are urged to submit their policies to the Office of the CIO Security Group, security@osu.edu, to assist in making users aware of what their department policies are and to provide examples that can be referenced by other areas. We will maintain a web site listing the current [Department Policies](#).

Failure to develop or enforce such policies may result in a charge of \$100 per incident if the number of incidents exceeds 10% of the maximum amount of usable address space on any subnet in a given billing cycle.

4. The university is responsible for Internet activity originating from campus; therefore all activity must be traceable to the system responsible for the activity. To identify the user(s) of the system all user access from and within OSUNet must be authenticated. The OSUNet authentication requirements are outlined in Section 7 of this document.

5. In order to determine whether the university network is being targeted, any *host* security *incident* must be reported to the Office of the CIO Security Group Incident Response Team (IRT) security@osu.edu.

6. For numerous reasons (e.g. email blacklists, site licensed content and software) unauthenticated mail relays, proxies and other mechanisms (e.g. formmail.pl cgi scripts) that can be abused to relay email or network connections are prohibited.

1.4 Monitoring of the Network

OIT reserves the right to monitor any network connected to OSUNet. This includes examining packet operational information to determine operational characteristics, such as protocol types, proper use of network addresses, traffic demand, etc. and the scanning of devices connected to identify security vulnerabilities in accordance with all applicable

legal regulations and the [*University Policy on Responsible Use of University Computing Resources*](#).

OIT also requires departments to allow echo request and echo reply response packets across the [*campus network address space*](#), except from the [*student-housing network address space \(RESNET\)*](#) to aid in central statistical and trouble shooting functions.

1.5 Protection of the Network

In a perceived emergency situation OIT may take immediate steps, including fully or partially blocking OSUNet access, to ensure the integrity of the university data network and systems, safeguard the health and safety of university community members and property, or protect the university from liability.

If an academic or administrative unit recognizes what they consider to be an emergency situation before OIT intervenes, they may take steps that they deem necessary to ensure the integrity of their local network.

In the event that a host is denied network access the administrator is to notify the Office of the CIO Security Group Incident Response Team (IRT) [*security@osu.edu*](mailto:security@osu.edu) with the pertinent information about the incident using the information requirements outlined in section 5.3 of this document, as a guide to provide the IRT information about the incident.

1.6 Campus Border Port Blocking

In order to protect OSUNet from the rest of the Internet or visa versa, the Director of Enterprise Networking in consultation with the Network Engineering and The Office of the CIO Security Group may set up blocks on specific ports at the OSUNet border. OIT will attempt to notify all DNAs before the blocks take effect, and will attempt to limit the amount of time these blocks are in place. A list of the ports currently blocked, and their review dates can be found at, [*What network traffic does the University block at the Internet border?*](#)

1.7 OSUNet Best Practices

[*<DHCP Best Practices>*](#)

[*Host Security Best Practices*](#)

[*Network Best Practices \(pdf\)*](#)

[*Password Best Practices \(pdf\)*](#)

1.8 OSUNet Principles

Note: Before purchasing network hardware, software or consultation services, departments are encouraged to consult with OIT Enterprise Networking (osunet@net.ohio-state.edu) to ensure OSUNet compatibility of their purchases.

1. The financial model for OSUNet is based on partial cost recovery therefore there will be a charge for at least one port in each building in which a department has a presence.
2. A department may request the aggregation of multiple buildings to a single OSUNet port. The Director of Enterprise Networking will review the request, and may approve it based on the technical requirements of the request. If the request is approved, the per building charges will continue to apply.
3. IPV4 is the standard communications protocol; IPV6 is available for non-production use.
4. No department devices will be connected directly to the OSUNet backbone.
5. In any location where OIT deploys services, including Public Computing Sites, the service is to be isolated from the rest of the building's network(s).
6. Excessive or abusive use of OSUNet bandwidth is not permitted. For example, excessive network traffic and spam are not permitted on OSUNet. Devices or networks may be blocked or disabled if necessary to protect the campus network, as outlined in section 1.4 of this document.
7. All users of OSUNet are responsible for following the Ohio State [Policy on Responsible Use of University Computing Resources](#).
8. Deployment of network wiring infrastructure within an academic or administrative unit must comply with the [Campus Wiring Standards](#).
9. Any unit that receives an OSUNet connection cannot also connect their local network with another ISP, service provider or other entity without prior written approval from the director of Enterprise Networking.
10. Prior approval is required by the Director of Enterprise Networking to deploy networking technologies that privately connect multiple physical locations at the Ohio State University. If the chosen method to interconnect multiple locations is the use of private fiber UNITS must also approve the deployment. Any unapproved installations may result in the termination of the OSUNet connection(s) at those location(s).

11. All wireless devices connected to OSUNet must comply with the [*Policy on Deployment and Use of Wireless Data Networks*](#).

1.9 References

OSUNet Connection request form

[*http://www.net.ohio-state.edu/OSUNet_Connection_Request.pdf*](http://www.net.ohio-state.edu/OSUNet_Connection_Request.pdf)

Minimum knowledge and skills a Department needs to receive an OSUNet connection

[*http://www.net.ohio-state.edu/dna/department.html*](http://www.net.ohio-state.edu/dna/department.html)

Minimum Expectations of DNAs

[*http://www.net.ohio-state.edu/dna/baselevel.html*](http://www.net.ohio-state.edu/dna/baselevel.html)

Hostmaster FAQ

[*http://www.net.ohio-state.edu/hostmaster*](http://www.net.ohio-state.edu/hostmaster)

Department Policies

[*TBD*](#)

University Policy on Responsible Use of University Computing Resources

[*http://cio.osu.edu/policies/responsible_use.html*](http://cio.osu.edu/policies/responsible_use.html)

The OSU Campus network address space

[*http://www.net.ohio-state.edu/subnets.html*](http://www.net.ohio-state.edu/subnets.html)

The student-housing network address space (RESNET)

[*http://www.net.ohio-state.edu/subnets.html#cat2*](http://www.net.ohio-state.edu/subnets.html#cat2)

What network traffic does the University block at the Internet border

[*http://www.net.ohio-state.edu/security/faqs/5.6.shtml*](http://www.net.ohio-state.edu/security/faqs/5.6.shtml)

DHCP Best Practices

[*TBD*](#)

Host Security Best Practices

[*http://www.net.ohio-state.edu/security/papers.shtml*](http://www.net.ohio-state.edu/security/papers.shtml)

Network Best Practices

[*http://www.net.ohio-state.edu/OSUNet/Network_Best_Practices.pdf*](http://www.net.ohio-state.edu/OSUNet/Network_Best_Practices.pdf)

Password Best Practices

[*http://www.net.ohio-state.edu/OSUNet/Password_Best_Practices.pdf*](http://www.net.ohio-state.edu/OSUNet/Password_Best_Practices.pdf)

Campus Wiring Standards

<http://units.osu.edu/vendors/index.html>

Policy on Deployment and Use of Wireless Data Networks

<http://cio.osu.edu/policies/wireless.html>

9. Glossary

Return to Index

2. Domain Name Service (DNS) Requirements

(The current DNS deployment is under review 5/3/04) This section will not be reviewed during the NETWOG meeting November 30, 2004

OIT Enterprise Networking maintains the OSUNet Domain Name Service (DNS) servers. All domains used to publish services external to the university must be housed on the OSUNet DNS servers.

All devices connected to OSUNet must be registered in the university DNS. To register a device the DNA for the network must submit email to the university hostmaster, (hostmaster@net.ohio-state.edu). To review the format guidelines required for DNS requests view the [Hostmaster FAQ](#).

OIT no longer delegates control of domains to academic or administrative units. Historically, a few entities at the university were delegated control when the original campus network was created, and they have been allowed to maintain control of their DNS. In order to manage their DNS these entities must continue to show that they have the technical ability and resources to properly manage their domains.

2.1 The osu.edu domain

The osu.edu name space has been opened up to academic or administrative units on campus on a case-by-case basis. The following rules govern its use:

1. The osu.edu domain is intended for short URL's to web sites. However to maintain a standard format all names are limited to < name>.osu.edu. To aid users that type www.<name>.osu.edu, a www.<name>.osu.edu record will be created to direct the user to the same server that houses the <name>.osu.edu site.

Email functionality for an approved <name>.osu.edu can be provided, if the DNA provides the information about the correct email server to the university hostmaster, (hostmaster@net.ohio-state.edu).

2. To provide everyone with an equal opportunity to request names and to provide a central reviewing body the [Web Policy Committee](#) has been asked to review and approve all names in the osu.edu name space.

3. All approved requests are maintained as aliases (CNAME records) to a server located in the department's ohio-state domain, and are required to be directed to a server on the university network.

2.2 The ohio-state.edu domain

All devices connected to OSUNet are to resolve to an academic or administrative unit's ohio-state.edu subdomain. The use of the ohio-state.edu domain is limited to devices that are connected to OSUNet.

If a department is interested in requesting a new subdomain name in the ohio-state.edu name space the DNA must fill out the [Subdomain Request form \(pdf\)](#) and document in a brief letter the intended use and number of *hosts* for the new subdomain.

2.3 Non ohio-state.edu domains

In those cases where the standard ohio-state and osu.edu domains do not reflect the purpose of a web site (e.g. a joint project with external organizations and /or universities) OIT will entertain requests for alternative domains and if approved, provide DNS hosting services for other Top Level Domains (TLDs).

If the TLD is not for an external project the domain needs to reflect in the name an association with the university.

Any group that requests a non-standard domain must show why the traditional ohio-state domain does not work for their situation. The requesting group also must demonstrate that the project supports the mission of the university.

After discussions on how the university is marketed with University Relations an agreement was reached that the .com TLD does not reflect how the university should be marketed. As a result OIT will not support DNS for .com TLD's. Additionally OIT will not allow the hosting of content that resolves with a .com TLD on the university network.

For a domain to be approved using one of the alternative TLDs, the requesting party must submit the following:

A letter on departmental letterhead signed by the unit chair/dean/director addressing the following:

1. A description of the purpose/function/nature of the organization that includes the participants involved (including physical locations for both the on and off campus parts of the organization) and the role the university plays in the organization.

a. If the university already provides hosting for other domains for the parties involved how the new domain differs from the existing domain(s).

2. Certifying that it is not a private business or other commercial venture.

3. Agreeing to a periodic review and renewal process of approved domains to insure that the content matches the original signed agreement and that no commercial activity is taking place.

4. Stating that they understand it is the organization's responsibility to incur any additional costs in the registration process, including but not limited to transferring or renewing the domain name registration with the appropriate domain registrar.

A second more technical letter from the DNA is also needed that addresses the following:

1. Indicating the billing contact in the organization.

2. Agreeing to coordinate the creation of the domain with OIT at Network Solutions, with the following conditions:

a. Agreeing that OIT will maintain the domain's primary and secondary name servers.

b. Agreeing that the "Administrative" and "Billing" contacts will be listed as someone in the requesting organization.

c. The "Registrant" and "Technical" contact information will be the registered NIC handle for the University, ZE146-ORG.

3. Providing the IP (s) that will be used with the new domain.

4. Agreeing that OIT will only support published domain names, and will not provide DNS for other domains that are variations of the published name. (e.g., Publishing <name>.org and asking for <name>.net to point to the same place.)

Both of these documents are to be mailed or faxed to the following:

Ohio State Hostmaster
320 West 8th Ave
Columbus, Ohio 43201-2331
614-292-9525 fax

2.4 Hosting DNS for TLDs on campus

OIT is responsible for all aspects of OSUNet including DNS. As a consequence, all TLD domains using university resources are required to reside on the OIT name servers.

Any domain that is found that was created without consulting OIT will be reviewed, and if it meets both the requirements for hosting and residing on the university network, it will be added to the OIT name servers after the department complies with the requirements outlined in Section 2.3 of this document. If a domain is discovered on the university network that does not meet the requirements set forth by OIT, it may be removed from OSUNet.

This also includes previously approved domains that did not continue their stated purpose, function, or nature of the domain.

2.5 Windows Active Directory and DNS

Enterprise Networking supports the records required by Microsoft active directory. However, due to the security issues that accompany allowing dynamic updates to the campus name servers, dynamic updating is not allowed.

The [Active Directory configuration page](#) explains DNS options for departments.

2.6 References

Hostmaster FAQ

<http://www.net.ohio-state.edu/hostmaster>

Web Policy Committee

<http://www.osu.edu/newmedia/>

Subdomain Request form

http://www.net.ohio-state.edu/OSUNet_Subdomain_Request.pdf

Active Directory configuration page

<http://www.net.ohio-state.edu/domainpolicy/adconfig.html>

9. Glossary

Return to Index

3. Host Security Requirements

The following requirements are the minimum steps that are to be taken to secure a *host* on OSUNet. However for some legacy hardware and operating systems not all of the

requirements can be followed. In those special situations the devices are not be connected to OSUNet unless placed behind a network based firewall and/or authentication mechanisms to meet the following requirements.

3.1 Installation Requirements

When installing a host on OSUNet, administrators are expected to adhere to the following list of best practices:

1. Installation of the host operating system and all applicable security patches must be done with the host disconnected from OSUNet, or otherwise isolated from all inbound network traffic.
2. Before the host is connected to a network, any services not used or required for operation must be disabled.
3. If a host-based firewall is available, it must be enabled before the host is connected to the network.

3.2 Password Requirements

Administrators must make sure that all administrative privileged accounts have strong passwords. If accounts have default passwords, they must be changed or the account completely disabled before a host is connected to the network. For more information on passwords, please review our [Password Best Practices \(pdf\)](#).

3.3 Antivirus Requirements

For operating systems for which the university owns site-licensed anti-virus software, these hosts at a minimum need to have real time virus scanning enabled, along with checking daily for updates to their virus library (e.g. daily DAT file downloads). Please see the [OSU Site Licensed Software](#).

3.4 Auditing Requirements

At least quarterly, systems connected to OSUNet must be audited for security vulnerabilities. Administrators responsible for their department network or machines may acquire software to do this auditing themselves, and the Office of the CIO Security Group may do separate audits on a as needed basis. Any vulnerabilities found must be corrected in a timely manner.

Administrators also need to review all system logs on a regular (at least weekly) basis. Logging requirements are outlined in Section 6 of this document.

3.5 Additional Host Security Information

The above outlined requirements are only the minimum standards, and should be considered a starting point for securing systems on OSUNet. For a more detailed discussion on system security, along with detailed best practices for a variety of operating systems, see the OSU [*Host Security Best Practices*](#).

3.6 References

Password Best Practices

http://www.net.ohio-state.edu/OSUNet/Password_Best_Practices.pdf

Site Licensed Software

<http://osusls.osu.edu/>

Host Security Best Practices

<http://www.net.ohio-state.edu/security/papers.shtml>

9. Glossary

Return to Index

4. Network Security Requirements

4.1 Authentication Requirements

All network access beyond the local network segment must be authenticated. An academic or administrative unit can choose to extend this requirement to include requiring authentication to access their local network segment.

Complete authentication requirements are outlined in Section 7 of this document, along with a list of acceptable forms of authentication.

4.2 Networking Devices

All networking devices must be configured to require strong passwords, and restrict management logins to OSUNet, the academic or administrative unit can choose to further restricted access to their network.

4.3 Additional Network Security Information

The above outlined requirements are only the minimum standards, and should be considered a starting point for securing a LAN on OSUNet. For a more detailed discussion on network security, along with detailed best practices see the <[OSUNet Network Security Best Practices](#)>.

4.4 References

OSUNet Network Security Best Practices
[TBD](#)

9. Glossary

[Return to Index](#)

5. Host Blocking and Unblocking Procedures

5.1 Notification about blocked hosts

When the Office of the CIO Security Group Incident Response Team (IRT) blocks an address of a *host*, the network contacts will be notified by e-mail, and by other means if practical. The network contacts are responsible for notifying the affected users, and either fixing the problem or passing the notification to the responsible parties so that they can address the problem. The following are guidelines when dealing with the IRT regarding blocked *hosts*.

5.2 Blocked Host Message

When the IRT sends out a notice about the blocking of a *host*, the message will include as much information as possible on the incident, along with instructions on how to have the *host* unblocked. To verify which *hosts* are blocked the IRT maintains a list only available from OSUNet at; <http://www.net.ohio-state.edu/security/restricted/BH/blackhole.cgi>

5.3 Unblocking a Host

To have a *host* unblocked, the administrator must send e-mail that includes the following items to security@osu.edu, which is the only group that can unblock a host.

1. The IP address and IRT incident number of the *host*.

2. An explanation of what was wrong with the host (found viruses, a backdoor, etc.).
3. How the problem was corrected.
4. If the incident was a result of a lack of patches or virus protection, a list of steps taken to prevent the recurrence of the infection need to be included. If steps are being taken but have not been deployed, to prevent a recurrence, please indicate them in your response.

The IRT would prefer that you reply to or forward a copy of the initial “block” e-mail complete with the original subject when requesting that a host be unblocked. Otherwise Failure to properly identify the host, the incident, and the steps taken to clean up and prevent recurrences may result in delays in unblocking the address.

5.4 Multiple Unblock Requests

If an administrator has multiple hosts to be unblocked as part of the same incident, they can be included in a list in a single e-mail that includes the incident number and IP addresses. However, failure to properly identify the hosts, the incident, and the steps taken to clean up and prevent recurrences may result in delays in unblocking the addresses.

If administrators have multiple hosts from different incidents, it will aid in the tracking of the individual incidents if the administrator sends separate e-mail replies to their respective block messages, including the steps taken to clean up and prevent recurrences.

5.5 Questions

If you have any security related questions send them to security@osu.edu. Please try to include the OSU-IRT incident number if your question pertains to a blocked host, or a particular incident.

5.6 References

Blocked hosts on OSUNet

<http://www.net.ohio-state.edu/security/restricted/BH/blackhole.cgi>

9. Glossary

Return to Index

6. Logging Requirements

University academic and administrative units are responsible for OSUNet traffic originating in the facilities and areas they administer, and are responsible for verifying that they can supply authentication logs for any lab or general use computers (including wireless access points) that are in their jurisdiction. Authentication requirements are outlined in Section 7 of this document.

All authentication, NAT translation and Dynamic Host Configuration Protocol (DHCP) logs must be kept a minimum of 30 days, but may be kept longer at the discretion of the unit.

Logs other than authentication, NAT translations and DHCP logs are often useful in diagnosing a problem, and should be kept for a minimum of 14 days.

6.1 References

DHCP Best Practices

[TBD](#)

9. Glossary

[Return to Index](#)

7. Authentication Requirements

7.1 Requirements

To help the university responsibly administer network traffic, all OSUNet access must be authenticated and logged.

All devices (including multi-user systems), where they have the technical capability, should be configured to authenticate users and keep the authentication logs for at least the minimum log period.

Authentication information (generally username and password information) must not be sent "in the clear" (unencrypted). Please see the [*Password Best Practices \(pdf\)*](#) for further information on how to protect your password information.

7.2 Acceptable Forms of Authentication

Many forms of authentication exist, the choice of the method is dependent on what the academic or administrative unit chooses to support. For central authentication the university supports Kerberos (name.n@osu.edu).

All computer labs, public or locked must authenticate users before they are allowed access beyond the local network. Guest account access should be disabled, so that authenticated access is the only access method allowed.

The only time physical access is an acceptable method of authentication is when it is used in conjunction with a private securable office, otherwise a technology similar to the following, or one of the following needs to be used and logged in accordance to the logging requirements outlined in Section 6 of this document.

- Biometrics
- Kerberos (name.n@osu.edu)
- MAC address
- Radius
- Windows Active Directory
- Windows NT Domain
- One time Passwords
- Token ID's (two factor authentication)

7.3 References

Password Best Practices

http://www.net.ohio-state.edu/OSUNet/Password_Best_Practices.pdf

9. Glossary

Return to Index

8. Enforcement

Enforcement of these technical standards depends on the severity of the infraction.

8.1 Incidents that require an active response

The following penalties will be levied in situations when a proactive response to protect OSUNet is warranted:

If a *host* shows a clear threat to OSUNet it will be removed from the network. Additional monetary penalties may be levied against the academic or administrative department if during the investigation it is discovered that they have not developed and enforced a policy to patch and maintain the *hosts* on their network in a timely way.

If a host is blocked from the network other issues for the host and or network will need to be resolved before the host is unblocked:

1. Any *host* that is blocked from the network and remains blocked in excess of 30 days may incur a daily fine of five dollars until the *OSU-IRT incident* is resolved.
2. If the network that a *host* resides on does not have on file the required secondary contact or a second DNA the host will not be unblocked until a secondary contact is registered.
3. If the number of incidents where a department's hosts are blocked exceeds 10% of the maximum number of usable address space on any subnet in a given billing cycle. a \$100 per incident fee may be incurred, as outlined in Section 1 of this document.

8.2 Incidents that do not require an active response

In situations that do not exhibit a direct threat to the operation of OSUNet, but a host or connection is not in compliance with the standards outlined in this document the following penalties:

Every OSUNet connection has a term of three years. During the renewal process updated contact and fiscal information must be provided for the network connection.

During the renewal process the unit's network will be audited for compliance with this policy and any outstanding issues will need to be resolved for the network connection to continue.

8.3 References

9. Glossary

Return to Index

9. Glossary

Bridging Firewall - A device that filters packets to a network as a bridge. This type of firewall is network architecture dependent. The advantages of a Bridging firewall are that it is easy to retrofit the firewall into an existing network without reconfiguring the workstations on the network. [Firewalls FAQ](#)

Desktop - A computer primarily used to provide direct access (via a locally attached keyboard, mouse and monitor) to applications such as web browsers, email clients, office productivity and data analysis tools for use usually by one individual at a time.

Firewall – A system designed to prevent unauthorized access to or from a local network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized access to networks or devices connected to the Internet. All traffic entering or leaving the local network passes through the firewall, which examines the traffic and blocks activity that does not meet the specified security criteria. [Firewalls FAQ](#)

Incident – A violation of an explicit or implied security policy. Of course, this definition relies on the existence of a security policy that, while generally understood, varies among organizations. These include but are not limited to attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data, changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

Network Address Translation - (NAT) is a way to map an entire network (or networks) to one or many IP address (es). NAT is usually used when the number of IP addresses assigned by an Internet Service Provider is less than the total number of computers that you wish to provide Internet access for. NAT is described in RFC 1631. The use of NAT on OSUNet is strongly discouraged, and should not be used for security purposes in a production environment. [Reasons not to use NAT](#)

OSU-IRT incident number – To assist the OSU incident response team in handling computer security and abuse investigations they create an incident number used to identify the parties involved. (ie: OSU-IRT#yyyy-mm-dd-001)

Routing Firewall - A device that becomes the default gateway or static route for network traffic to flow through. This type of firewall communicates with routers and shares routing information to help determine where the traffic should be routed and if the traffic should be passed. This often requires reconfiguration of network routers and workstations on the network. A [Firewalls FAQ](#) has been created to answer common questions about firewalls. This type of firewall should not be used on OSUNet, and may incur additional monthly fees to accommodate routing changes if it is installed

Server - A computer used primarily to provide network-based services (e.g. web, file, or email), for use typically by multiple users. Servers should not be used as a desktop machine and have a static network address.

Workstation - See Desktop.

Host – Any network-enabled device connected to the campus network. Examples include desktops, servers, workstations, printers, firewalls, network connected research instruments, information kiosks, and network switches.